Covering techniques in Integer & Lattice Programming

Moritz Venzin
École polytechnique fédérale de Lausanne
moritz.venzin@epfl.ch

I will present two ideas based on high-dimensional coverings that yield some of the currently best approximation algorithms for Integer & Lattice Programming. These problems are as follows: Given some convex body $K \subseteq \mathbb{R}^n$, is there an integer point in K? This problem is central in the algorithmic geometry of numbers and has found applications in Integer Programming and plays a key role in proposed schemes for post-quantum Cryptography. The following two natural geometric considerations have led to improvements in the current state-of-the-art algorithms for Lattice Programming:

- Given some convex body $K \subseteq \mathbb{R}^n$, how many convex bodies Q_i are required to cover K so that, when scaled around their respective centroids by a factor of 2, these convex bodies are contained inside $(1+\epsilon) \cdot K$? This question was first considered by Eisenbrand et al. in the context of Integer Programming for $K = B_\infty^n$. In that case, a simple dyadic decomposition along the facets reveals that $O(1+\log(1/\epsilon))^n$ convex bodies suffice. For general ℓ_p norm balls, exploiting the modulus of smoothness, $O(1+1/\epsilon)^{n/\min(p,2)}$ convex bodies suffice. This is tight for the Euclidean ball, but it is wide open whether for general K (even for the cross-polytope) there is an improvement over $O(1+1/\epsilon)^n$.

- Let K be some convex body and let $\mathcal{E}$ be some ellipsoid enclosing K. We consider the translative covering number $N(\mathcal{E}, K)$ but with a twist: For $\epsilon > 0$, is there some constant $C_\epsilon > 0$ so that $N(\mathcal{E}, C_\epsilon \cdot K) < 2^{\epsilon n}$? When $K = B_\infty^n$ and the ellipsoid is $\sqrt{n}B_2^n$, the answer is yes, i.e. for any $\epsilon > 0$, we can scale the cube by some constant and cover $\sqrt{n}B_2^n$ by fewer than $2^{\epsilon n}$ translates. Similarly, when K is the ℓ_p norm ball for $p \geq 2$ and the ellipsoid is an adequately scaled ball, the answer is yes, while for $p < 2$, the answer is no (compare the volume).

For both problems I will describe the techniques to obtain these results, briefly sketch their relevance to Lattice Programming and present some open questions. The talk is based on joint works with Márton Naszódi and Fritz Eisenbrand respectively.